

GIBSON, DUNN & CRUTCHER LLP
Orin Snyder (*pro hac vice*)
osnyder@gibsondunn.com
200 Park Avenue
New York, NY 10166-0193
Telephone: 212.351.4000
Facsimile: 212.351.4035

Kristin A. Linsley (SBN 154148)
klinsley@gibsondunn.com
Rosemarie T. Ring (SBN 220769)
rring@gibsondunn.com
Austin V. Schwing (SBN 211696)
aschwing@gibsondunn.com
Martie Kutscher (SBN 302650)
mkutscherclark@gibsondunn.com
555 Mission Street, Suite 3000
San Francisco, CA 94105-0921
Telephone: 415.393.8200
Facsimile: 415.393.8306

Attorneys for Defendant Facebook, Inc.,

GIBSON, DUNN & CRUTCHER LLP
Deborah Stein (SBN 224570)
dstein@gibsondunn.com
Heather L. Richardson (SBN 246517)
hrichardson@gibsondunn.com
333 South Grand Avenue
Los Angeles, CA 90071-3197
Telephone: 213.229.7000
Facsimile: 213.229.7520

Joshua S. Lipshutz (SBN 242557)
jlipshutz@gibsondunn.com
1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
Telephone: 202.955.8500
Facsimile: 202.467.0539

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

IN RE: FACEBOOK, INC. CONSUMER
PRIVACY USER PROFILE LITIGATION,

This document relates to:

ALL ACTIONS

CASE NO. 3:18-MD-02843-VC

**DEFENDANT'S STATEMENT IN
SUPPORT OF PLAINTIFF'S MOTION
FOR PRELIMINARY APPROVAL OF
CLASS ACTION SETTLEMENT**

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. SUMMARY OF PLAINTIFFS’ PRIORITIZED ALLEGATIONS.....	1
III. PLAINTIFFS FACE NUMEROUS SIGNIFICANT OBSTACLES IN LITIGATION	2
A. Plaintiffs’ “friend sharing” theory was largely dismissed, and the remainder of the claim is subject to significant defenses.....	3
B. Plaintiffs’ “whitelisting” theory faces substantial challenges.....	4
C. Plaintiffs’ “business partner” allegations face substantial obstacles.	6
D. Plaintiffs’ “enforcement” theory faces substantial obstacles.....	7
E. Plaintiffs’ VPPA claim faces substantial obstacles.	9
F. Plaintiffs’ SCA claim faces substantial obstacles.	11
G. Plaintiffs face serious challenges to establishing damages.....	11
H. Plaintiffs face serious challenges to establishing and maintaining class certification through trial.....	13
IV. CONCLUSION.....	14

TABLE OF AUTHORITIES**PAGE(S)****CASES**

<i>Carrera v. Bayer Corp.</i> , 727 F.3d 300 (3rd. Cir. 2013)	4, 14
<i>Cheung v. Wells Fargo Bank, N.A.</i> , 987 F. Supp. 2d 972 (N.D. Cal. 2013)	12
<i>Comcast Corp. v. Behrend</i> , 569 U.S. 27 (2013)	11, 12, 13
<i>In re Facebook Privacy Litig.</i> , 791 F. Supp. 2d 705 (N.D. Cal. 2011)	12
<i>In re Facebook, Inc., Sec. Litig.</i> , 477 F. Supp. 3d 980 (N.D. Cal. 2020)	8
<i>Gen. Bedding Corp. v. Echevarria</i> , 947 F.2d 1395 (9th Cir. 1991)	3
<i>Hanlon v. Chrysler Corp.</i> , 150 F.3d 1011 (9th Cir. 1998)	1
<i>In re Hulu Privacy Litig.</i> , No. C 11-03764 LB, 2014 WL 1724344 (N.D. Cal. Apr. 28, 2014)	10
<i>Illinois v. Facebook, Inc.</i> , 2018 CH 3868 (Cir. Ct. Cook Cnty., Ill. Mar. 8. 2021)	8
<i>Lindsey v. Normet</i> , 405 U.S. 56 (1972)	14
<i>Nalbandyan v. Citibank, NA</i> , 777 F. App'x 189 (9th Cir. 2019)	9
<i>Poulos v. Caesars World, Inc.</i> , 379 F.3d 654 (9th Cir. 2004)	8
<i>Santa Barbara v. Super. Ct.</i> , 41 Cal. 4th 747 (2007)	8, 9
<i>Schofield v. Delta Air Lines, Inc.</i> , No. 18-CV-00382-EMC, 2019 WL 955288 (N.D. Cal. Feb. 27, 2019)	1
<i>Tenet Healthsystem Desert, Inc. v. Blue Cross of California</i> , 245 Cal. App. 4th 821	5

1	<i>Vasquez v. Coast Valley Roofing, Inc.</i> ,	
2	670 F. Supp. 2d 1114 (E.D. Cal. 2009).....	1
3	<i>Velasquez v. Centrome, Inc.</i> ,	
4	233 Cal. App. 4th 1191 (2015)	9
5	<i>In re Vizio, Inc., Consumer Priv. Litig.</i> ,	
6	238 F. Supp. 3d 1204 (C.D. Cal. 2017)	9, 10
7	<i>Wal-Mart Stores, Inc. v. Dukes</i> ,	
8	564 U.S. 338 (2011)	4, 8
9	<i>Zepeda v. PayPal, Inc.</i> ,	
10	777 F. Supp. 2d 1215 (N.D. Cal. 2011)	7
11	STATUTES	
12	18 U.S.C. § 2702(b)(3).....	6
13	18 U.S.C. § 2710(a)(3).....	5
14	18 U.S.C. § 2710(a)(4).....	4
15	18 U.S.C. § 2710(b)(1).....	5
16	Cal. Civ. Code §§ 1698 (b), (c).....	5
17	TREATISES	
18	Restatement (Third) of Restitution and Unjust Enrichment § 51(5).....	7

I. INTRODUCTION

The Cambridge Analytica events and extensive news coverage surrounding them sparked several investigations and lawsuits about Facebook’s data-sharing practices, including this MDL. The data-sharing practices underlying those events no longer exist, and other practices challenged by Plaintiffs are now governed by comprehensive privacy and enforcement programs subject to oversight by the Federal Trade Commission. *See* Elia Decl. (Dkt. 1094); Dunphy Decl. (Dkt. 1095).

After more than four years of litigation, which included extensive fact discovery spanning a fifteen-year period, this MDL has been resolved through a proposed settlement which, if approved, would provide substantial compensation to the settlement class and avoid the risk, expense, and uncertainty of further litigation for all parties. As Plaintiffs explain in their motion for preliminary approval (“Motion”), the proposed settlement is fair, adequate, and reasonable, and “the size of the Settlement,” which is unprecedented, “is even more striking in light of the risks [Plaintiffs and the putative class] faced.” Dkt. 1096 at 14. Facebook respectfully submits this statement in support of Plaintiffs’ Motion to provide further detail regarding these risks which are among the most significant considerations in determining whether to grant preliminary approval under Rule 23(e). *See generally* *Hanlon v. Chrysler Corp.*, 150 F.3d 1011, 1026 (9th Cir. 1998); *Schofield v. Delta Air Lines, Inc.*, No. 18-CV-00382-EMC, 2019 WL 955288, at *4 (N.D. Cal. Feb. 27, 2019); *Vasquez v. Coast Valley Roofing, Inc.*, 670 F. Supp. 2d 1114, 1125–26 (E.D. Cal. 2009).

II. SUMMARY OF PLAINTIFFS’ PRIORITIZED ALLEGATIONS

Plaintiffs filed this case in 2018, following press around the alleged improper use of Facebook user data by Cambridge Analytica, a British political consulting firm. In violation of Facebook’s policies, Cambridge Analytica purchased that user data from a Cambridge University researcher named Aleksandr Kogan who had obtained that data from users who installed an app he created on Facebook’s platform and opted to share data for limited purposes. The Named Plaintiffs are friends of users who installed Kogan’s app and alleged they did not understand that an early version of Facebook’s Platform allowed app developers (like Kogan) to request data about them through their Facebook friends, if their privacy settings allowed it.

Through numerous complaints culminating in a First Amended Consolidated Complaint, Plaintiffs broadly alleged that Facebook shared user data with app developers and other third parties without consent or sufficient disclosure and did not sufficiently monitor third parties' use of user data or compliance with its data use policies. On September 9, 2019, the Court issued an order granting in part and denying in part Facebook's motion to dismiss Plaintiffs' First Amended Consolidated Complaint, identifying the following four categories of alleged misconduct that would move forward to discovery: **(1) Friend sharing.** Plaintiffs alleged that Facebook did not adequately disclose that the first version of Facebook's app-developer Platform (Graph API V.1) allowed apps (like Kogan's) to request data about users through their friends. Dkt. 298 at 6–7. The Court held that Facebook's friend sharing disclosures were sufficient at least as early as 2009, leaving open a question as to whether Facebook's earliest users consented to friend sharing. *Id.* at 25–27. **(2) Whitelisting.** Plaintiffs alleged that Facebook told users in 2014 that it was terminating friend sharing but then allowed a select group of "whitelisted" apps to continue accessing friends' data in violation of users' expectations and in exchange for advertising revenue. *Id.* at 7–8. **(3). Business partners.** Plaintiffs alleged that Facebook maintained data-sharing arrangements with a broad range of "partners" that were premised on "data reciprocity" agreements and not disclosed to users. *Id.* at 8. **(4). Enforcement.** Plaintiffs alleged that Facebook did not sufficiently monitor third parties' use of user data or enforce third-party compliance with Facebook's data use policies. *Id.* at 9-10.

Based on these four categories of alleged misconduct, the Court allowed Plaintiffs to pursue, on a prioritized basis, California contract and tort claims. It also permitted Plaintiffs to move forward with federal statutory claims under the Video Privacy Protection Act and Stored Communications Act.

III. PLAINTIFFS FACE NUMEROUS SIGNIFICANT OBSTACLES IN LITIGATION

The Motion discusses risks Plaintiffs face in proving their claims and establishing liability on a class-side basis. These risks, and others, are discussed below in more detail and show the significant hurdles Plaintiffs would face in proving allegations underlying each category of alleged misconduct, many of which Facebook contends were not borne out in discovery.

A. Plaintiffs’ “friend sharing” theory was largely dismissed, and the remainder of the claim is subject to significant defenses.

Plaintiffs allege that Facebook violated a promise that users could “control how [their data] is shared” by failing to disclose “friend sharing,” which allowed third-party apps on the first version of Facebook’s Graph API platform to request certain data about users through friends who installed these apps. Based on friend-sharing disclosures in Facebook’s Data Use Policies effective in 2009 and after, the Court allowed only users who joined Facebook before 2009 to pursue claims based on this theory. Dkt. 298 at 25–27. Because friend-sharing disclosures in Facebook’s Data Use Policies before 2009 were materially the same but not before the Court at the motion-to-dismiss stage, the remaining pre-2009 claims would also have been subject to dismissal on the same grounds. *Id.* at 27. Discovery confirmed that Facebook began disclosing friend sharing in 2007 (when Facebook released its developer Platform), in nearly identical language to the 2009 disclosure the Court found sufficient. Facebook’s May 24, 2007 Privacy Policy states: “If you, *your friends*, or members of your network use any third-party applications developed using the Facebook Platform (‘Platform Applications’), those Platform Applications may access and share certain information about you with others in accordance with your privacy settings.” Dkt. 187-34 at 6 (*italics added*). Facebook believes this disclosure would defeat Plaintiffs’ friend-sharing theory for users who joined Facebook between 2007 and 2009.

Facebook would also argue that Plaintiffs’ friend-sharing claims are time-barred, regardless of when users joined Facebook. The longest limitations period for Plaintiffs’ surviving claims is four years (breach of written contract), and the limitations period “begins to run[] when [a party] has actual or constructive notice of its claims.” *Gen. Bedding Corp. v. Echevarria*, 947 F.2d 1395, 1397 (9th Cir. 1991) (*emphasis omitted*). As discussed above, Facebook publicly disclosed friend sharing in 2007, more than a decade before Plaintiffs filed this case.

Even if friend sharing were a viable theory of liability, Plaintiffs would have faced substantial evidentiary obstacles in proving what, if any, non-public sensitive data was shared with third parties for particular users without consent. *See* Dkt. 1096 at 21. Third parties made data requests from Facebook through “API calls.” But there are insufficient records showing what user data third parties requested through API calls during the time when friend sharing existed, what data was returned in

response to those requests, and the privacy settings on that data. Without such evidence, Plaintiffs would have to prove liability by relying on “general practices,” *id.*, and a chain of inferences that non-public sensitive data was shared with third parties *for all users* without their consent, which Facebook would argue are unsupported and do not satisfy Plaintiffs’ burden of proof. A class-wide liability finding based on such inferences would also be precluded by the Rules Enabling Act and Due Process. *See Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 366–67 (2011) (the Due Process Clause and the Rules Enabling Act forbid the application of different substantive rules in class actions); *Carrera v. Bayer Corp.*, 727 F.3d 300, 307 (3rd. Cir. 2013) (“A defendant in a class action has a due process right to raise individual challenges and defenses to claims, and a class action cannot be certified in a way that eviscerates this right or masks individual issues.”).

B. Plaintiffs’ “whitelisting” theory faces substantial challenges.

Plaintiffs allege that Facebook deceived users by allowing certain “whitelisted” apps to continue to request user data through their friends (allegedly in exchange for advertising revenue) despite a statement by Mark Zuckerberg at Facebook’s annual f8 developer conference in April 2014 that Facebook was planning to transition away from friend sharing: “[W]e are going to make it so that now, everyone has to choose to share their own data with an app themselves.” *See* Dkt. 491 (SACC) ¶ 441. Plaintiffs assert claims for breach of contract and deceit by concealment because Facebook did not end friend sharing for all apps immediately after the f8 conference and instead allowed for a one-year transition period for the vast majority of apps and then whitelisted a small subset of apps to allow continued access to friends’ data.¹

Plaintiffs face significant hurdles to establishing liability on their whitelisting theory. *See* Dkt. 1096 at 29. The f8 conference is an event at which Facebook announces changes to developers who understand it takes time to implement these changes. Indeed, the statement at issue did not represent that all friend sharing would end immediately, and, despite Plaintiffs’ allegations of nefarious motives, there were legitimate reasons for whitelisting based on user experiences and unique constraints, including allowing time to redesign apps. *See* Dkt. 1038-16 at 199:22–200:12.

¹ As Steven Elia describes in his declaration, Dkt. 1094, friend sharing was ended years ago.

For Plaintiffs’ deceit by concealment claim, in addition to demonstrating that users heard (or read about) the statement at the f8 conference, Plaintiffs would also have to prove that users would have acted differently had they known about whitelisting (Dkt. 1096 at 29), that Facebook intentionally hid from users (with the intent to defraud them) that friend sharing would not end immediately after the f8 conference, and that users had no knowledge of the ongoing friend sharing. *See* Dkt. 298 at 37; *see also Tenet Healthsystem Desert, Inc. v. Blue Cross of California*, 245 Cal. App. 4th 821, 844. Plaintiffs would face significant obstacles establishing these facts. No evidence was uncovered in discovery showing any of the Plaintiffs heard the f8 conference statements, let alone relied on them. Further, even after the 2014 developer conference, Facebook continued to disclose, and users continued to consent to, “friend-sharing” through Facebook’s Data Use Policy, disproving the factual basis of Plaintiffs’ claim and creating a statute-of-limitations issue. *See* Dkt. 298 at 22 (“[U]sers agreed to substantially similar language between roughly 2009 and 2015.”); Dkt. 187-47 at 3 [January 30, 2015 Data Use Policy] (“In some cases, people you share and communicate with may download or re-share this content with others on and off our services.” “[W]hen you download or use such third-party services, they can access your Public Profile, . . . your list of friends, as well as any information that you share with them.”); Dkt. 187-48 at 4 [September 29, 2016 Data Policy] (same).

With respect to Plaintiffs’ contract-based claims, Plaintiffs cannot rely on statements made at a developer conference (much less statements they did not hear) to change the terms of their contractual agreements with Facebook. *See* Cal. Civ. Code §§ 1698 (b), (c) (“A contract in writing may be modified by an oral agreement” only if it is “executed by the parties” and “supported by new consideration”). As for damages, Plaintiffs acknowledge that “Facebook could contest the connection between the [alleged] contractual breaches and its revenue. And even if that connection were established, Facebook could challenge the amount by which relevant third parties would have decreased their advertising spend [if they had not been whitelisted].” Dkt. 1096 at 23. As discussed below, *see infra* at p. 12, if litigation continued, Facebook would demonstrate that whitelisting decisions were not based on advertising revenue.

Finally, Plaintiffs’ whitelisting theory faces the same evidentiary hurdles in proving that non-

public sensitive data was shared with third parties for any particular user without consent, particularly since only a small fraction of apps were whitelisted. *See supra* at pp. 3-4.

C. Plaintiffs’ “business partner” allegations face substantial obstacles.

Plaintiffs’ “business partner” theory is based on allegations that Facebook entered into undisclosed “data reciprocity” arrangements under which “Facebook and its partners agreed to exchange information about users’ activities with each other.” Dkt. 491 ¶ 434; Dkt. 298 at 8. There is no evidence that Facebook maintained data reciprocity arrangements with any third party, and Facebook would argue Plaintiffs’ business partner claims (including their contract, tort, and statutory claims) fail for this reason alone. For “integration partners,” with which Facebook partnered to make Facebook and certain Facebook functionalities available on certain early smartphones, operating systems, and internet platforms, Facebook would point to clear disclosures throughout the class period that certain data was shared with “service providers” and “third-party integrations,” as well as direct consents by users to share data with these third parties. *See, e.g.* Dkt. 187-45 at 16 [December 11, 2012 Data Policy] (“Service Providers: We give your information to the people and companies that help us provide, understand, and improve the services we offer. For example, we may use outside vendors to help host our website.”); Dkt. 187-47 at 3 [January 30, 2015 Data Policy] (“Apps, websites and third-party integrations on or using our Services . . . may receive information about what you post or share”); *see also* Dkt. 187-48 at 4 [September 29, 2016 Data Policy] (same). These disclosures and consents also provide a statute-of-limitations defense. *See supra* at p. 3.

Throughout this litigation, Plaintiffs argued their “business partner” theory also includes allegations that Facebook’s relationships with advertisers and data brokers wrongly subjected them to “psychographic marketing.” *See* Dkt. 491 ¶ 270; *see* Dkt. 762-3 at 169-171 (ECF pagination) (arguing business partners include advertisers and data brokers). In its order on Facebook’s motion to dismiss, the Court observed that these advertising-based theories were “quite vague” and included no “meaningful explanation of the legal or factual difference between psychographic marketing and targeted advertising,” which “the plaintiffs appear to concede is perfectly legitimate.” Dkt. 298 at 5–6. Discovery confirmed that Facebook did not provide user-identified data to advertisers or data

1 brokers that could have been used to target or deliver ads in the way Plaintiffs allege, and Facebook's
2 own use of user data for advertising was disclosed. Facebook informed users as early as 2009: "We
3 allow advertisers to choose the characteristics of users who will see their advertisements and we may
4 use any of the non-personally identifiable attributes we have collected (including information you may
5 have decided not to show other users, such as your birth year or other sensitive personal information
6 or preferences) to select the appropriate audience for those advertisements." Dkt. 187-39 at 4
7 [December 9, 2009 Privacy Policy]. Facebook also disclosed that it received data from third parties to
8 assist with ad placement. Beginning in 2011, under the heading "Other information we receive about
9 you," Facebook's Data Use Policy stated: "Sometimes we get data from our advertising partners,
10 customers and other third parties that helps us (or them) deliver ads, understand online activity, and
11 generally make Facebook better." Dkt. 187-43 at 2 [September 7, 2011 Data Use Policy].

12 Finally, as with Plaintiffs' other theories, even if Plaintiffs' allegations about Facebook's
13 "business partners" were true, which they are not, there are no records available showing what if any
14 information was received by third parties, let alone that such data included non-public sensitive user
15 data shared without consent.

16 **D. Plaintiffs' "enforcement" theory faces substantial obstacles.**

17 If this litigation were to proceed, Plaintiffs would rely on documents from Facebook's App
18 Developer Investigation, which focused on app activity prior to 2014, to prove breach-of-contract and
19 negligence claims based on monitoring and enforcement efforts. Dkt. 1096 at 21. Facebook would
20 argue that identifying examples of pre-2014 platform violations cannot prove Plaintiffs' claims.

21 ***Breach of contract.*** Plaintiffs allege that Facebook maintained a contractual obligation to
22 monitor and prevent data misuse by app developers because its Data Use Policy stated: "If an
23 application asks permission from someone else to access your information, the application will be
24 allowed to use that information only in connection with the person that gave the permission and no one
25 else." See Dkt. 298 at 28. Plaintiffs argue evidence showing specific third parties did not comply with
26 this policy proves Facebook violated this provision. Dkt. 1096 at 21.

27 Facebook would argue that a reasonable person would not have understood the language
28

Plaintiffs point to as a promise by Facebook to guarantee that every app complied with its policies, and instead would have understood the language to state a rule for app developers to follow. Other courts have agreed with this reading. *See Illinois v. Facebook, Inc.*, 2018 CH 3868, at *11 (Cir. Ct. Cook Cnty., Ill. Mar. 8. 2021); *In re Facebook, Inc., Sec. Litig.*, 477 F. Supp. 3d 980, 1021 (N.D. Cal. 2020).

As one court explained:

[Facebook’s representation in its Data Use Policy] does not provide a plausible basis to co[n]clude that a reasonable person reading these policies might believe that their data was guaranteed to be safe from third-party app developers, especially third-party developers who might violate Facebook’s Data Use Policy. Instead, Facebook repeatedly states in its policies that it is not responsible for the actions of third parties....

Illinois, 2018 CH 3868, at *11.

In fact, Facebook’s policies expressly advised that it could not guarantee apps would follow its rules or that Facebook would catch every violation of its policies:

You should always review the policies of third party applications and websites to make sure you are comfortable with the ways in which they use information you share with them. We do not guarantee that they will follow our rules.

Dkt. 187-41 at 4 [(Oct. 5, 2010 Privacy Policy) (emphasis added). Facebook further advised: “We do our best to keep Facebook safe, but we cannot guarantee it,” Dkt. 187-26 [SRR, § 3 (Jan. 30, 2015), and “FACEBOOK IS NOT RESPONSIBLE FOR THE ACTIONS, CONTENT, INFORMATION, OR DATA OF THIRD PARTIES.” Dkt. 187-23 [SRR, § 16(3) (June 8, 2012)].

Facebook’s disclosures pose a substantial risk to Plaintiffs’ theory that Facebook had a contractual obligation to guarantee apps followed its rules. Even if Plaintiffs could establish such an obligation, any contractual breach resulting in misuse of sensitive data by third parties could not be shown on a class-wide basis.

Negligence. Users’ contractual agreements with Facebook release claims for ordinary negligence. *See* Dkt. 298 at 36; *see also* Dkt. 1096 at 7. As a result, to prove liability Plaintiffs would have to prove *gross negligence*. To do so, Plaintiffs would be required to prove a breach of care so severe as to evidence “a want of even scant care or an extreme departure from the ordinary standard of conduct.” *Santa Barbara v. Super. Ct.*, 41 Cal. 4th 747, 754 (2007). While Facebook has undoubtedly made significant improvement to its monitoring and enforcement efforts over the last decade,

1 “[t]he standard of care . . . under California law is established by looking to the industry customs and
 2 practices in effect at the time.” *Nalbandyan v. Citibank, NA*, 777 F. App’x 189, 191 n. 1 (9th Cir.
 3 2019); *Velasquez v. Centrome, Inc.*, 233 Cal. App. 4th 1191, 1216 (2015) (to establish negligence, the
 4 plaintiff must prove a departure from “the standard of care in the . . . industry at the time.”).

5 Facebook would present evidence that, in the absence of any regulatory regime or industry
 6 standard governing how Facebook should conduct Platform enforcement, Facebook led the industry in
 7 developing a monitoring and enforcement program from the ground up more than 15 years ago, and
 8 utilized extensive automated and manual app review processes, a standardized enforcement rubric,
 9 confidential user reports, tips from employees and third parties, and external security vendors. No
 10 monitoring program of millions of apps could possibly catch every potential Platform violation, and
 11 Facebook’s early program was not without flaws. But, in light of the efforts Facebook made to develop
 12 a novel monitoring and enforcement program, Plaintiffs face a significant risk that they would be
 13 unable to demonstrate Facebook acted without “even slight care,” or in “an extreme departure from the
 14 ordinary standard of conduct.” *Santa Barbara*, 41 Cal. 4th at 765.

15 **E. Plaintiffs’ VPPA claim faces substantial obstacles.**

16 Plaintiffs identify several risks they face under the VPPA, including the statute’s two-year
 17 limitations period, whether any data Facebook shared constitutes “personally identifiable data” as that
 18 term is defined by the VPPA, a lack of records reflecting what (if any) data was actually shared, and
 19 due process considerations. Dkt. 1096 at 23-26. These are not the only risks.

20 *First*, Plaintiffs would also have to establish that Facebook is a “video tape service provider”
 21 (“VTSP”) under the VPPA. A VTSP is an entity that is “engaged in the business . . . of rental, sale, or
 22 delivery of prerecorded video cassette tapes or similar audio visual materials” 18 U.S.C.
 23 § 2710(a)(4). Courts have interpreted and applied this defined term to mean a business that is not only
 24 “substantially involved in the conveyance of video content to consumers but also *significantly tailored*
 25 *to serve that purpose.*” *In re Vizio, Inc., Consumer Priv. Litig.*, 238 F. Supp. 3d 1204, 1221 (C.D. Cal.
 26 2017) (emphasis added). This excludes entities that are only “peripherally or passively involved.” *Id.*
 27 at 1221-22.

Facebook would argue that it is not the type of entity Congress intended the VPPA to regulate. Congress passed the VPPA in response to a local video store disclosing Supreme Court nominee Robert Bork's family's video rental history to a reporter. *In re Hulu Privacy Litig.*, No. C 11-03764 LB, 2014 WL 1724344, at *8 (N.D. Cal. Apr. 28, 2014). Unlike a video store or even a modern-day video streaming service, Facebook is a platform that allows users to deliver different types of content, including videos, to other users. Facebook would argue that it is not a VTSP because it is only "passively involved" with the delivery of video content and its business is not "significantly tailored" for that purpose. Instead, it is a platform by which users deliver their own content to other users of their choice. *See Vizio*, 238 F. Supp. 3d at 1221-22.

Second, a party is liable under the VPPA only if it shares "personally identifiable information" about video-watching behavior without consent. The statute does not apply where there has been no disclosure of a person's video-watching history that can be identified to a specific person. Plaintiffs would face significant hurdles proving this element. *See* Dkt. 1096 at 24.

Under the VPPA, "personally identifiable information" is "information which identifies a person as having requested or obtained specific video materials or services from a [VTSP]." 18 U.S.C. § 2710(a)(3). But apps have never had the ability to request data about what videos users have watched on the Facebook platform. Plaintiffs claim the VPPA applies because some third parties have had access to users' "likes" and "comments" on videos posted to Facebook and they believe it can be inferred that a user who liked or commented on a video watched it. But many users have never engaged with video content on Facebook at all, and users often like or comment on content (including videos) merely because the content was posted by a friend or family member, or because they were tagged in the post. Users can engage with video content in this manner, without ever watching the video. Facebook would argue the VPPA does not reach these scenarios.

Third, Facebook would argue that when a user engages in a social action such as liking or commenting on a video, Facebook is not the entity "disclos[ing]" that information to third parties as the VPPA requires. *See* 18 U.S.C. § 2710(b)(1). The *user* themselves discloses the information by posting a like or comment on someone else's video, and the user who posted the content decides the

audience for the video and any likes or comments on it. Facebook does not make that decision. Facebook’s privacy policy has consistently disclosed that if a user likes or comments on another user’s post, the user who posted the video can make that like or comment available to anyone else, including making the post public. *See, e.g.* Dkt. 187-44 at 6 [June 8, 2012 Data Use Policy] (“When you comment on or ‘like’ someone else’s story, or write on their timeline, that person gets to select the audience. For example, if a friend posts a Public story and you comment on it, your comment will be Public. Often, you can see the audience someone selected for their story before you post a comment; however, the person who posted the story may later change their audience.”); Dkt. 187-49 [July 24, 2018 Data Policy]. This is far different than the sort of private video rental scenario that gave rise to the VPPA.

F. Plaintiffs’ SCA claim faces substantial obstacles.

Plaintiffs also face risks on their Stored Communications Act claim, given the statute requires only single party consent to share an electronic communication. 18 U.S.C. § 2702(b)(3); *see also* Dkt. 1096 at 26-27. Plaintiffs’ SCA theory is largely tied to allegations that users did not sufficiently consent to third parties accessing communications with their friends that their friends chose to share. Under these circumstances, the SCA’s consent requirement would be satisfied. Plaintiffs do not contend, nor is there evidence to show, that Facebook shared communications with third parties without consent from any party to the communication.

G. Plaintiffs face serious challenges to establishing damages.

In addition to risks on liability issues, Plaintiffs also face risks in proving damages (particularly on a class wide basis), given that (i) Facebook is a free service (Dkt. 1096 at 14), and (ii) Plaintiffs’ unjust enrichment theory is subject to several defenses (*id.* at 22).

As for damages, in its motion to dismiss order, the Court held Plaintiffs did not “plausibly allege” that they suffered any “economic loss” as a result of the alleged misconduct, and Plaintiffs had alleged at most an “intangible injury” from the unauthorized “disclosure of sensitive private information.” Dkt. 298 at 13-14, 42. Plaintiffs have not provided a damages theory tied to this intangible harm, and Facebook would argue Plaintiffs could not do so on a class-wide basis in a manner that complies with the Supreme Court’s decision in *Comcast Corp. v. Behrend*, 569 U.S. 27, 35 (2013).

1 Plaintiffs have instead focused largely on an unjust enrichment theory of damages, seeking
 2 disgorgement of Facebook’s revenues attributable to advertising. But disgorgement is not an available
 3 remedy because Plaintiffs did not convey anything of value to Facebook. Dkt. 1096 at 22. Facebook
 4 would also argue that Plaintiffs may not pursue unjust enrichment because “a quasi-contract action for
 5 unjust enrichment” is not available where a contract governs the parties’ relationship. *In re Facebook*
 6 *Privacy Litig.*, 791 F. Supp. 2d 705, 718 (N.D. Cal. 2011); *see Cheung v. Wells Fargo Bank, N.A.*, 987
 7 F. Supp. 2d 972, 979 (N.D. Cal. 2013); *Zepeda v. PayPal, Inc.*, 777 F. Supp. 2d 1215, 1223 (N.D. Cal.
 8 2011). Here, Plaintiffs alleged, and the Court agreed, that “[a]t all relevant times, Facebook and
 9 Plaintiffs mutually assented to, and therefore were bound by . . . Facebook’s Statement of Rights and
 10 Responsibilities or later, the Terms of Service.” Dkt. 491 ¶ 883.

11 As Plaintiffs explain, even if disgorgement were available, they would face significant obstacles
 12 establishing a *direct causal connection* (as required) between their data-sharing claims and Facebook’s
 13 advertising revenue. Dkt. 1096 at 22; *see also Am. Master Lease LLC v. Idanta Partners, Ltd.*, 225
 14 Cal. App. 4th 1451, 1491 (2014) (disgorgement requires a determination of “the net profit attributable
 15 to the underlying wrong”); Restatement (Third) of Restitution and Unjust Enrichment § 51(5)
 16 (recognizing that the court may “apply such tests of causation and remoteness”). Facebook would
 17 present evidence that the data-sharing theories at issue in this case are separate from Facebook’s
 18 advertising business, and (as discussed above) Facebook has not shared user-identified data with
 19 advertisers.² Plaintiffs have claimed Facebook whitelisted certain entities so that they would continue
 20 to purchase advertising on Facebook. Facebook would contest that assertion and present evidence
 21 showing the vast majority of Facebook’s ad revenue was generated by advertisers not affected by
 22 whitelisting, multiple third parties whose apps were whitelisted did not advertise on Facebook at all,
 23 and Facebook even saw *decreases* in ad revenue from several whitelisted entities during the time their
 24 apps were whitelisted. Facebook would also argue that Plaintiffs cannot establish a class wide damages
 25 model, as there is no data from which they could tie specific amounts of “unjustly gained” advertising
 26

27 ² If the same entity is an app developer and an advertiser, that entity may receive user data in con-
 28 nection with its app.

revenue to data shared improperly on behalf of the entire class. *Comcast*, 569 U.S. at 35.

In light of these considerations, even if Plaintiffs prevailed on any of their claims, they faced a significant risk that any damages awarded would be limited to nominal damages, which would be less than the settlement amount. *See* Dkt. 1096 at 28-30.

H. Plaintiffs face serious challenges to establishing and maintaining class certification through trial.

Plaintiffs would face significant obstacles on class certification issues. While Plaintiffs acknowledge this risk for some of their claims, Dkt. 1096 at 36, Facebook would argue that none of Plaintiffs' claims are amenable to class treatment because they turn on individualized issues, including: (1) a user's expectation of privacy based on their exposure to disclosures, experiences on Facebook and other social media, and privacy settings; (2) whether a user posted or shared sensitive information on Facebook and related privacy settings; and (3) whether any non-public sensitive information posted or shared by a user was shared with third parties without the user's consent. Similarly, determining whether a user's sensitive data was shared with third parties depends on a series of individualized issues, including: (1) a user's friends over time; (2) which apps a user's friends installed; (3) the types of data the friends' apps had permission to receive for a user and the user's friends; (4) what data requests each of the friends' apps actually made and what information was returned; and (5) whether any information returned to the app was "sensitive" and non-public.

If litigation were to continue, Facebook would oppose class certification because each of these issues would require individualized proof. *Comcast*, 569 U.S. at 34. Plaintiffs have suggested they could overcome this risk by asking the fact finder to "infer" that all class members were harmed because user data was widely shared with third parties. Facebook would argue that such an inference could not satisfy Plaintiffs' burden of proof and would be impermissible under the Due Process Clause and Rules Enabling Act, which forbid the application of different substantive rules in class actions, including evidentiary rules that eliminate a defendant's ability to present individualized defenses that would otherwise be available in an individual action. *See Dukes*, 564 U.S. at 366–67; *Poulos v. Caesars World, Inc.*, 379 F.3d 654, 664 (9th Cir. 2004) (Rule 23 cannot alter plaintiffs' burden of proof);

1 *Lindsey v. Normet*, 405 U.S. 56, 66 (1972) (“Due process requires that there be an opportunity to
2 present every available defense.”); *Carrera*, 727 F.3d at 307 (“A defendant in a class action has a due
3 process right to raise individual challenges and defenses to claims, and a class action cannot be certified
4 in a way that eviscerates this right or masks individual issues.”).

5 **IV. CONCLUSION**

6 For these reasons, and those set forth in the Motion, the proposed \$725 million settlement is
7 fair, reasonable, and adequate, and warrants preliminary approval. Facebook reserves all rights to
8 respond to any objections and/or opposition to the Motion.

9 Dated: January 18, 2023

GIBSON, DUNN & CRUTCHER LLP

10
11 By: Rosemarie T. Ring

12 Rosemarie T. Ring

13 *Attorneys for Defendant Facebook, Inc.*
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28